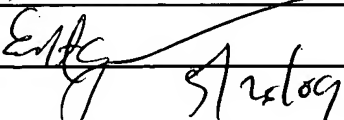
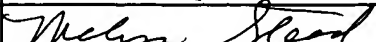
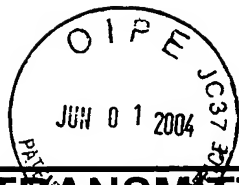


TRANSMITTAL FORM <i>(to be used for all correspondence after initial filing)</i>		Application No.	10/750,516
		Filing Date	December 31, 2002
		First Named Inventor	Dae-Ha Lee
		Art Unit	
		Examiner Name	
Total Number of Pages in This Submission	6	Attorney Docket Number	3364P160

ENCLOSURES (check all that apply)		
<input checked="" type="checkbox"/> Fee Transmittal Form <input type="checkbox"/> Fee Attached <input type="checkbox"/> Amendment / Response <input type="checkbox"/> After Final <input type="checkbox"/> Affidavits/declaration(s) <input type="checkbox"/> Extension of Time Request <input type="checkbox"/> Express Abandonment Request <input type="checkbox"/> Information Disclosure Statement <input type="checkbox"/> PTO/SB/08 <input checked="" type="checkbox"/> Certified Copy of Priority Document(s) <input type="checkbox"/> Response to Missing Parts/Incomplete Application <input type="checkbox"/> Basic Filing Fee <input type="checkbox"/> Declaration/POA <input type="checkbox"/> Response to Missing Parts under 37 CFR 1.52 or 1.53	<input type="checkbox"/> Drawing(s) <input type="checkbox"/> Licensing-related Papers <input type="checkbox"/> Petition <input type="checkbox"/> Petition to Convert a Provisional Application <input type="checkbox"/> Power of Attorney, Revocation Change of Correspondence Address <input type="checkbox"/> Terminal Disclaimer <input type="checkbox"/> Request for Refund <input type="checkbox"/> CD, Number of CD(s)	<input type="checkbox"/> After Allowance Communication to Group <input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences <input type="checkbox"/> Appeal Communication to Group (Appeal Notice, Brief, Reply Brief) <input type="checkbox"/> Proprietary Information <input type="checkbox"/> Status Letter <input checked="" type="checkbox"/> Other Enclosure(s) (please identify below): <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> Request for Priority; return postcard </div>
Remarks		

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT	
Firm or Individual name	Eric S. Hyman, Reg. No. 30,139 BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Signature	
Date	5/26/04

CERTIFICATE OF MAILING/TRANSMISSION			
I hereby certify that this correspondence is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.			
Typed or printed name	Melissa Stead		
Signature		Date	5-26-04



IFW

FEE TRANSMITTAL for FY 2004

Effective 01/01/2004. Patent fees are subject to annual revision.

☒ Applicant claims small entity status. See 37 CFR 1.27.

TOTAL AMOUNT OF PAYMENT (\$)

Complete if Known

Application Number 10/750,516
Filing Date December 31, 2002
First Named Inventor Dae-Ha Lee
Examiner Name
Art Unit
Attorney Docket No. 3364P160

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None
☒ Deposit Account

Deposit Account Number

02-2666

Deposit Account Name

Blakely, Sokoloff, Taylor & Zafman LLP

The Commissioner is authorized to: (check all that apply)

☒ Charge fee(s) indicated below ☐ Credit any overpayments
☒ Charge any additional fee(s) or underpayment of fees as required under 37 CFR §§ 1.16, 1.17, 1.18 and 1.20.
☐ Charge fee(s) indicated below, except for the filing fee to the above-identified deposit account

FEE CALCULATION

1. BASIC FILING FEE

Large Entity		Small Entity		Fee Description	Fee Paid
Fee Code	Fee (\$)	Fee Code	Fee (\$)		
1001	770	2001	385	Utility filing fee	
1002	340	2002	170	Design filing fee	
1003	530	2003	265	Plant filing fee	
1004	770	2004	385	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	
SUBTOTAL (1)					

2. EXTRA CLAIM FEES

Total Claims - 20 = X =
Independent Claims - 3 = X =
Multiple Dependent

Large Entity		Small Entity		Fee Description	Fee Paid
Fee Code	Fee (\$)	Fee Code	Fee (\$)		
1202	18	2202	9	Claims in excess of 20	
1201	86	2201	43	Independent claims in excess of 3	
1203	290	2203	145	Multiple Dependent claim, if not paid	
1204	86	2204	43	**Reissue independent claims over original patent	
1205	18	2205	9	**Reissue claims in excess of 20 and over original patent	
SUBTOTAL (2)					

**or number previously paid, if greater. For Reissues, see below

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity		Small Entity		Fee Description	Fee Paid
Fee Code	Fee (\$)	Fee Code	Fee (\$)		
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet.	
2053	130	2053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for ex parte reexamination	
1804	920 *	1804	920 *	Requesting publication of SIR prior to Examiner action	
1805	1,840 *	1805	1,840 *	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	420	2252	210	Extension for reply within second month	
1253	960	2253	475	Extension for reply within third month	
1254	1,480	2254	740	Extension for reply within fourth month	
1255	2,010	2255	1,005	Extension for reply within fifth month	
1404	330	2401	165	Notice of Appeal	
1402	330	2402	165	Filing a brief in support of an appeal	
1403	290	2403	145	Request for oral hearing	
1451	1,510	2451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive - unavoidable	
1453	1,330	2453	665	Petition to revive - unintentional	
1501	1,330	2501	665	Utility issue fee (or reissue)	
1502	480	2502	240	Design issue fee	
1503	640	2503	320	Plant issue fee	
1460	130	2460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	770	1809	385	Filing a submission after final rejection (37 CFR § 1.129(a))	
1810	770	2810	385	For each additional invention to be examined (37 CFR § 1.129(b))	
1801	770	2801	385	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	
Other fee (specify)					

* Reduced by Basic Filing Fee Paid

SUBTOTAL (3) (\$)

SUBMITTED BY

Complete (if applicable)

Name (Print/Type) Eric S. Hyman

Registration No. (Attorney/Agent)

30,139

Telephone

(310) 207-3800

Signature

Date

5/21/04

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:

DAE-HA LEE, ET AL.

Application No.: 10/750,516

Filed: December 31, 2002

For: Method for Creating and Verifying Simple
Object Access Protocol Message in Web Service
Security Using Signature Encryption

Art Group:

Examiner:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REQUEST FOR PRIORITY

Applicant respectfully requests a convention priority for the above-captioned application,
namely:

COUNTRY	APPLICATION NUMBER	DATE OF FILING
Korea	2003-0070551	10 October 2003

☒ A certified copy of the document is being submitted herewith.

Respectfully submitted,

Blakely, Sokoloff, Taylor & Zafman LLP

Dated: 5/26/04Eric S. Hyman, Reg. No. 30,13912400 Wilshire Boulevard, 7th Floor
Los Angeles, CA 90025
Telephone: (310) 207-3800

I hereby certify that this correspondence is being deposited with the United
States Postal Service on the date shown below with sufficient postage as first
class mail in an envelope addressed to: Commissioner for Patents, P.O. Box
1450, Alexandria, VA 22313-1450.

Melissa Stead
Melissa Stead5-26-04
Date

대한민국 특허청

KOREAN INTELLECTUAL
PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto
is a true copy from the records of the Korean Intellectual
Property Office.

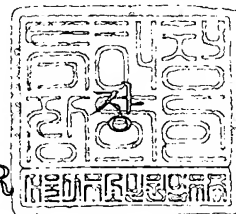
출원번호 : 10-2003-0070551
Application Number

출원년월일 : 2003년 10월 10일
Date of Application OCT 10, 2003

출원인 : 한국전자통신연구원
Applicant(s) Electronics and Telecommunications Research Ins-

2004 년 02 월 09 일

특허청
COMMISSIONER



【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0001
【제출일자】	2003.10.10
【발명의 명칭】	서명 암호화를 이용한 웹서비스 보안에서의 SOAP 메시지 생성 및 검증 방법
【발명의 영문명칭】	METHOD FOR CREATING AND VERIFYING SIMPLE OBJECT ACCESS PROTOCOL MESSAGE ON WEB SERVICE SECURITY USING SIGNATURE ENCRYPTION
【출원인】	
【명칭】	한국전자통신연구원
【출원인코드】	3-1998-007763-8
【대리인】	
【명칭】	유미특허법인
【대리인코드】	9-2001-100003-6
【지정된변리사】	이원일
【포괄위임등록번호】	2001-038431-4
【발명자】	
【성명의 국문표기】	이대하
【성명의 영문표기】	LEE,DAE H
【주민등록번호】	711119-1673813
【우편번호】	305-350
【주소】	대전광역시 유성구 가정동 236-1번지 ETRI 기숙사 구관 108호
【국적】	KR
【발명자】	
【성명의 국문표기】	박찬규
【성명의 영문표기】	PARK,CHAN KYU
【주민등록번호】	700528-1683212
【우편번호】	302-781
【주소】	대전광역시 서구 만년동 상록수아파트 101동 1502호
【국적】	KR

【발명자】

【성명의 국문표기】 김록원
【성명의 영문표기】 KIM, ROCK WON
【주민등록번호】 730224-1673722
【우편번호】 305-350
【주소】 대전광역시 유성구 가정동 236-1번지 2동 232호
【국적】 KR

【발명자】

【성명의 국문표기】 문진영
【성명의 영문표기】 MOON, JIN YOUNG
【주민등록번호】 771230-2019041
【우편번호】 704-140
【주소】 대구광역시 달서구 이곡동 성서우방타운 101동 201호
【국적】 KR

【발명자】

【성명의 국문표기】 송병열
【성명의 영문표기】 SONG, BYOUNG YOUL
【주민등록번호】 730120-1409021
【우편번호】 305-755
【주소】 대전광역시 유성구 어은동 한빛아파트 129동 1502호
【국적】 KR

【발명자】

【성명의 국문표기】 정승우
【성명의 영문표기】 JUNG, SEUNG WOO
【주민등록번호】 750718-1852521
【우편번호】 305-752
【주소】 대전광역시 유성구 송강동 청솔아파트 206동 604호
【국적】 KR

【발명자】

【성명의 국문표기】 조현규
【성명의 영문표기】 CHO, HYUN KYU
【주민등록번호】 620126-1849919

【우편번호】	302-861
【주소】	대전광역시 서구 탄방동 1255 35/1
【국적】	KR
【발명자】	
【성명의 국문표기】	함호상
【성명의 영문표기】	HAM,HO SANG
【주민등록번호】	550320-1163126
【우편번호】	305-755
【주소】	대전광역시 유성구 어은동 한빛아파트 119동 303호
【국적】	KR
【심사청구】	청구
【취지】	특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사를 청구합니다. 대리인 유미특허법인 (인)
【수수료】	
【기본출원료】	20 면 29,000 원
【가산출원료】	9 면 9,000 원
【우선권주장료】	0 건 0 원
【심사청구료】	11 항 461,000 원
【합계】	499,000 원
【감면사유】	정부출연연구기관
【감면후 수수료】	249,500 원
【기술이전】	
【기술양도】	희망
【실시권 허여】	희망
【기술지도】	희망
【첨부서류】	1. 요약서·명세서(도면)_1통

【요약서】**【요약】**

본 발명은 서명 암호화를 이용한 웹서비스 보안에서의 SOAP 메시지 생성 및 검증 방법에 관한 것이다. SOAP 메시지 송신자는 SOAP 본문(Body)에 들어갈 데이터를 암호화하는 비밀키를 사용하여 SOAP 메시지 보안에 사용되는 서명을 암호화한다. 암호화된 서명은 SOAP 헤더(Header)의 보안 헤더에 삽입되어 수신자에게 전송된다. SOAP 메시지 수신자는 자신의 개인키를 사용하여 암호 키를 복호화한 후 비밀키를 복원한다. 복원된 비밀키는 SOAP 헤더의 보안 헤더 내에 있는 암호화된 서명을 복호화하는데 사용되고, 이렇게 복호화된 서명을 통해 SOAP 메시지가 검증된다. 본 발명에 따르면, SOAP 메시지에 기반한 웹서비스 SOAP 메시지에 대한 서명 암호화를 수행함으로써, SOAP 메시지 보안에 기초한 웹서비스 보안에서 발생할 수 있는 잠재적인 서명 위조의 위험을 효과적으로 막을 수 있다.

【대표도】

도 6

【색인어】

웹서비스 보안, SOAP 메시지 보안, 보안 헤더, 인증, 서명 암호화, 비밀키, 대칭 암호 알고리즘, 비대칭 암호 알고리즘, XML

【명세서】**【발명의 명칭】**

서명 암호화를 이용한 웹서비스 보안에서의 SOAP 메시지 생성 및 검증 방법{METHOD FOR CREATING AND VERIFYING SIMPLE OBJECT ACCESS PROTOCOL MESSAGE ON WEB SERVICE SECURITY USING SIGNATURE ENCRYPTION}

【도면의 간단한 설명】

도 1은 일반적인 SOAP 메시지의 구성도이다.

도 2는 도 1에 도시된 암호 키(Encrypted Key) 생성 메커니즘에 대한 블록도이다.

도 3은 도 1에 도시된 SOAP 메시지를 생성하는 흐름도이다.

도 4는 도 1에 도시된 SOAP 메시지를 수신측에서 수신하여 검증하는 과정을 나타낸 흐름도이다.

도 5는 일반적인 SOAP 메시지 보안에서 서명 위조 발생을 개략적으로 도시한 도면이다.

도 6은 본 발명의 실시예에 따른 서명 암호화를 이용한 웹서비스 보안 방법에서의 SOAP 메시지의 구성도이다.

도 7은 도 6에 도시된 암호화된 서명 생성 메커니즘에 대한 블록도이다.

도 8은 도 6에 도시된 SOAP 메시지를 생성하는 흐름도이다.

도 9는 도 6에 도시된 SOAP 메시지를 수신측에서 수신하여 검증하는 과정을 나타낸 흐름도이다.

**【발명의 상세한 설명】****【발명의 목적】****【발명이 속하는 기술분야 및 그 분야의 종래기술】**

- <10> 본 발명은 웹서비스 보안에 관한 것으로, 특히 SOAP(Simple Object Access Protocol) 메시지에 대한 보안(SOAP Message Security)에 중점을 둔 웹서비스 보안시 서명 암호화를 이용하여 SOAP 메시지를 생성하고 검증하는 방법에 관한 것이다.
- <11> 일반적으로 웹 서비스 보안은 SOAP 메시지에 대한 보안(SOAP Message Security)에 중점을 두고 있는데, 여기서 SOAP은 XML(eXtensible Markup Language)과 HTTP(HyperText Transfer Protocol) 통신을 기반으로 하여 네트워크 상에 존재하는 각종 컴포넌트간의 호출을 효율적으로 실현하기 위한 방법을 제시하는 규약이다. 이러한 SOAP은 메시지 기반 프로토콜이기 때문에 두 시스템간의 통합 시 쌍방간의 메시지 포맷만을 약속하면 되므로 통합시간 및 효율을 높일 수 있으며, 그 구조가 매우 간단하다는 특징을 가지고 있다.
- <12> SOAP 메시지 보안에서는 데이터의 무결성과 데이터에 대한 신원 확인을 위해 디지털 서명(Digital Signature)을 사용하고, 데이터에 대한 기밀성을 위해 데이터에 대한 암호화를 수행한다. 거기다가 데이터 암호화에 사용된 비밀키를 보호하기 위해 수신자의 공개키로 그 비밀키를 암호화하는 과정도 수행된다.
- <13> SOAP 메시지 보안을 포함한 웹서비스 보안 메커니즘은 기존에 존재하는 다양한 보안 모델과 암호 기술을 수용하는 형태로 설계된다. 이는 또한 보안 토큰에 대한 일반적인 메커니즘을 제공한다. 웹서비스 보안은 특별한 형태의 보안 토큰에 구애받지 않고, 다양한 형태의 보안 토큰에 적합하게 확장 가능한 형태로 설계된다. 이러한 웹서비스 보안 메커니즘은 부가적

으로 보안 토큰을 어떻게 인코딩할 것인지에 대해서도 기술하고 있는데, 특별히 규격에서는 X.509 인증서와 Kerberos Ticket에 대한 인코딩 방법을 기술하고 있으며, 암호화된 키를 어떻게 포함할 것인지에 대해서도 기술하고 있다.

<14> 웹서비스 보안과 관련된 기술로는 대한민국 특허공개번호 제2003-5675호(웹 모듈 인증 장치 및 방법)이 있는데, 이 기술은 웹 서비스를 개시하기 전에 인증서버를 통해 웹 모듈을 인증한 후 웹모듈의 인증이 확인된 경우에 한해서 서비스를 시작하여 웹모듈의 보안성을 증대시키는 것을 특징으로 한다.

<15> 그러나, 상기한 종래 기술들에서는 SOAP 메시지 전송 중에 제3자가 디지털 서명을 손쉽게 변경하거나 교체하여 서명 위조를 할 수 있다는 문제점이 있다.

<16> 따라서, 웹서비스 보안 기술에서 발생할 수 있는 서명 위조를 방지할 수 있는 방안이 요구된다.

【발명이 이루고자 하는 기술적 과제】

<17> 따라서, 본 발명의 기술적 과제는 상기한 문제점을 해결하고자 하는 것으로, SOAP 메시지 보안에 기초한 웹서비스 보안에서 데이터에 대한 무결성 및 신원 확인을 위한 서명문을 암호화하여 SOAP 메시지를 전송함으로써 제3자에 의한 서명 위조를 방지하는 서명 암호화를 이용한 웹서비스 보안에서의 SOAP 메시지 생성 및 검증 방법을 제공하는 것이다.

【발명의 구성 및 작용】

<18> 상기 과제를 달성하기 위한 본 발명의 하나의 특징에 따른 서명 암호화를 이용한 웹서비스 보안시 SOAP 메시지 생성 방법은,

- <19> SOAP(Simple Object Access Protocol) 메시지-여기서 SOAP 메시지는 보안 헤더 (Security Header)를 포함하는 SOAP 헤더(Header)와 SOAP 본문(Body)으로 이루어진 SOAP 봉투 (Envelope)를 포함함- 보안에 기초한 웹서비스 보안시 송신자에 의한 상기 SOAP 메시지 생성 방법으로서,
- <20> a) 상기 SOAP 메시지의 보안 정보의 재사용을 방지하기 위해 사용되는 타임스탬프 (Timestamp) 및 상기 SOAP 메시지의 보안 관련 정보인 보안 토큰(Security Token)을 생성하여 상기 SOAP 헤더의 보안 헤더에 삽입하는 단계; b) 상기 SOAP 메시지를 통해 송신될 데이터를 특정 비밀키를 사용하여 암호화하여 암호 데이터를 생성한 후 상기 SOAP 본문에 삽입하는 단계 ; c) 상기 SOAP 메시지에 대한 무결성 및 신원 확인을 위해 디지털 서명을 수행하여 서명문을 생성하고, 상기 생성된 서명문을 상기 특정 비밀키를 사용하여 암호화하여 암호화된 서명을 생성한 후 상기 SOAP 헤더의 보안 헤더에 삽입하는 단계; 및 d) 상기 데이터와 서명문의 암호화에 사용된 상기 비밀키를 상기 SOAP 메시지의 수신자의 공개키로 암호화하여 암호 키를 생성한 후 상기 SOAP 헤더의 보안 헤더에 삽입하는 단계를 포함한다.
- <21> 여기서, 상기 b) 단계 및 c) 단계에서, 상기 데이터 및 서명문의 암호화는 대칭키 암호 알고리즘에 따라 수행되는 것이 바람직하다.
- <22> 또한, 상기 d) 단계에서, 상기 비밀키의 암호화는 비대칭키 암호 알고리즘에 따라 수행 되는 것이 바람직하다.
- <23> 본 발명의 다른 특징에 따른 서명 암호화를 이용한 웹서비스 보안시 SOAP 메시지 검증 방법은,



- <24> SOAP(Simple Object Access Protocol) 메시지-여기서 SOAP 메시지는 보안 헤더 (Security Header)를 포함하는 SOAP 헤더(Header)와 SOAP 본문(Body)으로 이루어진 SOAP 봉투 (Envelope)를 포함함- 보안에 기초한 웹서비스 보안시 수신자에 의한 상기 SOAP 메시지 검증 방법으로서,
- <25> a) 상기 SOAP 메시지의 서명을 검증하기 위한 인증서를 획득하는 단계; b) 상기 수신자의 공개키로 상기 SOAP 헤더의 보안 헤더 내에 있는 암호 키를 복호화하여 비밀키를 획득하는 단계; c) 상기 획득한 비밀키를 사용하여 상기 SOAP 헤더의 보안 헤더 내에 있는 암호화된 서명을 복호화한 후 본래의 서명문을 복원하는 단계; d) 상기 a) 단계에서 획득한 인증서를 사용하여 상기 c) 단계에서 복원된 서명을 검증하는 단계; e) 상기 b) 단계에서 획득한 비밀키를 사용하여 상기 SOAP 본문에 있는 암호 데이터를 복호화한 후에 본래의 데이터를 복원하는 단계를 포함한다.
- <26> 여기서, 상기 a) 단계에서 상기 인증서는 상기 SOAP 헤더의 보안 헤더 내에 있는 보안 토큰(Security Token)에서 획득되는 것이 바람직하다.
- <27> 또한, 상기 c) 단계 및 e) 단계에서, 상기 암호화된 서명 및 암호 데이터의 복호화는 대칭키 암호 알고리즘에 따라 수행되는 것이 바람직하다.
- <28> 또한, 상기 b) 단계에서, 상기 암호 키의 복호화는 비대칭키 암호 알고리즘에 따라 수행되는 것이 바람직하다.
- <29> 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지



않는다. 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였다. 명세서 전체를 통하여 유사한 부분에 대해서는 동일한 도면 부호를 붙였다.

- <30> 이하, 첨부된 도면을 참조하여 본 발명의 실시예에 따른 서명 암호화를 이용한 웹서비스 보안 방법에 대해서 상세하게 설명한다.
- <31> 도 1은 일반적인 SOAP 메시지의 구성도이다.
- <32> 도 1에 도시된 바와 같이, SOAP 메시지는 두 개의 데이터 구조인 SOAP 헤더 (Header)(120)와 SOAP 본문(Body)(160)을 포함하는 SOAP 봉투(Envelope)(100)로 이루어진다.
- <33> SOAP 봉투(100)는 SOAP 메시지의 내용이나 주체 등에 대한 것을 나타내기 위한 전체적인 프레임워크(framework)를 제공한다.
- <34> SOAP 헤더(120)는 SOAP 메시지의 수신지와 송신지에 대한 정보를 나타내는 라우팅 정보 (Routing Information)(122)와 SOAP 보안을 위한 보안 헤더(Security Header)(140)를 포함한다 .
- <35> 보안 헤더(140)는 다시 타임스탬프(Timestamp)(142), 보안 토큰(Security Token)(144), 암호 키(Encrypted Key)(146) 및 서명(Signature)(148)을 포함한다.
- <36> 타임스탬프(142)는 보안 정보의 재사용을 방지하기 위해 사용되며, 보안 정보의 생성시간 및 유효기간 등으로 구성된다.
- <37> 보안 토큰(144)은 보안에 관련된 정보로서, 이는 다시 서명되지 않은 보안 토큰 (Unsigned Security Token)과 서명된 보안 토큰(Signed Security Token) 두 가지로 나뉜다. 서명되지 않은 보안 토큰은 인증기관에 의해 승인되지 않은 보안 토큰으로서, 보안 등급이 낮은 경우에 적용할 수 있는 정보로, 예를 들어 사용자 이름(Username) 등을 들 수 있다. 한편,



서명된 보안 토큰(Signed Security Token)은 인증기관에 의해 승인되고, 그 인증기관에 의해 암호학적으로 서명되어진 보안 토큰으로서, 이에는 X.509 인증서나 Kerberos Ticket 등이 있다

- <38> 암호 키(146)는 SOAP 본문(160)에 위치하는 데이터를 암호화한 비밀키(세션 키)가 수신자의 공개키로 암호화된 것을 말한다. 이는 SET(Secure Electronic Transaction)에서 사용된 전자 봉투와 같은 개념이다.
- <39> 서명(148)은 XML 디지털 서명 알고리즘을 이용하여 데이터를 서명한 부분으로 데이터의 무결성과 부인 방지 기능을 제공한다.
- <40> 한편, SOAP 본문(160)은 암호 데이터(Encrypted Data)(162)를 포함하며, 이 암호 데이터(162)는 XML 암호 알고리즘(Encryption Algorithm)을 이용하여 SOAP 본문 데이터를 암호화한 부분으로 데이터의 기밀성을 제공한다.
- <41> 도 2는 도 1에 도시된 암호 키(Encrypted Key)(146) 생성 메커니즘에 대한 블록도로, 암호 키 생성 메커니즘은 SOAP 메시지 보안에서 데이터를 암호화한 비밀키를 수신자의 공개키로 암호화해서 안전하게 전송하기 위한 메커니즘이다.
- <42> 이 메커니즘에서 비밀키(Secret Key)는 대칭키 암호 알고리즘에 사용되는 키를 말한다. 대칭키 암호 알고리즘에서는 암호화나 복호화시에 같은 키를 사용한다. 따라서 암호/복호화를 수행하기 앞서 키 교환 과정이 먼저 수행되어야 한다.
- <43> 한편, 개인키/공개키(Private Key/Public Key)는 비대칭키 암호 알고리즘에 사용되는 키들을 말한다. 비대칭키 암호 알고리즘에서는 암호화시에는 공개키를 사용하고 복호화시에는 개인키를 사용한다. 비대칭키 암호 알고리즘은 대칭키 암호 알고리즘과는 달리 암호/복호화 수



행 전에 키 교환 과정이 필요 없다. 또한 암호화시에 사용되는 공개키는 인증기관을 통해 외부에 공개되어지고, 복호화에 사용할 개인키는 개인이 소유하고 있으면 된다. 따라서, 비대칭 키 암호 알고리즘에서는 대칭 키 암호 알고리즘에서와 같이 키 교환 과정에서 키 분실에 대한 우려는 고려하지 않아도 된다.

<44> 세션키(Session Key)는 일정기간 동안 사용하기 위해 만들어진 키를 말하는 것으로, 키 재사용 방지를 위해 사용되어지며, 주로 대칭 키 암호 알고리즘에서 사용되어지는 비밀키를 세션키와 같은 형태로 만들어 사용한다.

<45> 도 2에 도시된 바와 같이, 암호 키 생성 메커니즘은 SET에서의 전자 봉투 메커니즘을 따랐는데, 일반적으로 데이터 내용이 긴 SOAP 본문 데이터는 암호/복호화 속도가 빠른 대칭 키 암호 알고리즘에 따라 비밀키(세션키)(220)를 사용하여 암호화(201)된 후 암호 데이터(162)로 만들어져 SOAP 본문(160)에 삽입된다(202). 여기서 사용된 비밀키(세션키)(220)는 비대칭 키 암호 알고리즘에 따라 수신자의 공개키(210)로 암호화(203)되어 일종의 전자봉투라 할 수 있는 암호 키(146)로 생성되어 SOAP 헤더(120), 특히 보안 헤더(Security Header)(140)에 삽입된다(204).

<46> 한편, SOAP 메시지 수신자는 자신의 개인키로 보안 헤더(140)의 암호 키(146)에 있는 암호화된 비밀키를 복호화해서 비밀키(세션키)(220)를 얻은 다음, 이 비밀키(세션키)(220)로 SOAP 본문(160)에 있는 암호 데이터를 복호화해서 SOAP 본문 데이터를 얻게 된다.

<47> 이 때, 비밀키(세션키)는 그 길이가 길지 않기 때문에 비대칭 키 암호 알고리즘으로 암호/복호화 하는데 많은 시간이 걸리지 않는다. 예를 들어, DES(Data Encryption Standard)의 경우에는 비밀키의 길이는 64비트이고, SSL(Secure Sockets Layer)의 경우에는 40-128비트 이내의 비밀키(세션키)를 사용한다.

- <48> 도 3은 도 1에 도시된 SOAP 메시지를 생성하는 흐름도이다.
- <49> 도 3을 참조하면, 먼저 SOAP 본문(160)에 실어 보낼 데이터를 생성한 후, SOAP 메시지 수신자에 대한 라우팅 정보를 구성하여 SOAP 헤더(120)의 라우팅 정보(122)를 생성한다(S310).
- <50> 다음, 보안 헤더(140)의 타임스탬프(142) 및 보안 토큰(144)를 생성한다(S320, S330). 이 때 보안 토큰(144)이 서명된 보안 토큰(Signed Security Token)인 경우엔 인증기관(Certification Authority)에 의뢰하여 얻을 수도 있다. 만약 SOAP 본문 데이터에 제3자에게 공개해서는 안 되는 정보가 있다면, 데이터를 암호화(S340)하여 암호 데이터(162)를 생성하여 SOAP 본문(160)에 삽입함으로써 SOAP 본문 데이터의 기밀성을 유지한다. 여기서, 암호화 과정은 XML 암호 알고리즘을 따른다.
- <51> 다음, 데이터 암호화에 사용된 비밀키(220)는 수신자의 공개키로 암호화하여 암호 키(146)를 생성한 후 보안 헤더(140)에 삽입한다(S350).
- <52> 마지막으로 데이터에 대한 무결성 및 신원확인을 위해 디지털 서명(Signature)을 행하여 보안 헤더(140)에 삽입한다(S360). 이 때 디지털 서명은 XML 디지털 서명 알고리즘에 의해 수행된다.
- <53> 도 4는 도 1에 도시된 SOAP 메시지를 수신측에서 수신하여 검증하는 과정을 나타낸 흐름도이다.
- <54> 도 4를 참조하면, 먼저 수신자는 전자 서명을 검증하기 위해 SOAP 메시지 헤더(120)나 외부의 인증기관으로부터 인증서를 얻은 후(S410), 해당 인증서를 가지고 SOAP 헤더(120) 내에 있는 보안 헤더(140)의 서명(148)을 검증한다(S420).



- <55> 서명이 검증되고 나면, 암호화된 데이터를 복호화하기 위해, 수신자의 개인키로 보안 헤더(140)의 암호 키(146)를 복호화하여 비밀키(220)를 획득한 후(S430), 획득된 비밀키(220)로 SOAP 본문(160)의 암호 데이터(162)를 복호화하여 본래의 데이터를 복원한다(S440).
- <56> 도 5는 일반적인 SOAP 메시지 보안에서 서명 위조 발생을 개략적으로 도시한 도면이다.
- <57> 도 5에 도시된 바와 같이, SOAP 메시지(520)의 송신자인 앨리스(Alice)는 SOAP 본문(524) 내에 암호화된 데이터 $ED(=Enc(Data))$ (524)를 서명하여 SOAP 헤더(522) 내에 $Sig_Alice(ED)$ (522)를 삽입하여 생성된 SOAP 메시지(520)를 수신자인 밥(Bob)에게 전송한다.
- <58> 이 때 오스카(Oscar)는 앨리스에서 밥으로 SOAP 메시지가 전송되는 전송로 상에서 앨리스가 보낸 SOAP 메시지(520)를 가로채서, 앨리스에 의해 서명된 부분인 $Sig_Alice(ED)$ (522)를 자신의 서명인 $Sig_Oscar(ED)$ (544)로 교체한 후, 오스카는 수정된 SOAP 메시지(540)를 다시 밥에게 보낸다.
- <59> 밥은 오스카에 의해 수행된 서명 위조 사실을 모른 채, 수신 받은 SOAP 메시지(560)가 앨리스가 아닌 오스카에 의해 서명되었다고 생각하게 된다.
- <60> 따라서, 오스카는 암호화된 데이터를 복호화할 필요 없이 중간에서 서명을 교체하여 위조함으로써 원래 데이터에 서명한 사람인 것처럼 위장할 수 있게 된다.
- <61> 이와 같이, SOAP 메시지 보안에 기초한 웹서비스 보안에서는 오스카와 같은 제3자가 전송되는 SOAP 메시지를 가로채 서명을 위조할 수 있다는 문제점이 있다.
- <62> 상기한 문제점은 이하 기술되는 본 발명의 실시예에 의해 극복될 수 있다.
- <63> 도 6은 본 발명의 실시예에 따른 서명 암호화를 이용한 웹서비스 보안 방법에서의 SOAP 메시지의 구성도이다.



- <64> 도 6에 도시된 바와 같이, 본 발명의 실시예에 따른 SOAP 메시지는 두 개의 데이터 구조인 SOAP 헤더(Header)(620)와 SOAP 본문(Body)(660)을 포함하는 SOAP 봉투(Envelope)(600)로 이루어진다.
- <65> SOAP 봉투(600)는 SOAP 메시지의 내용이나 주체 등에 대한 것을 나타내기 위한 전체적인 프레임워크(framework)를 제공하고, SOAP 헤더(620)는 SOAP 메시지의 수신지와 송신지에 대한 정보를 나타내는 라우팅 정보(Routing Information)(622)와 SOAP 보안을 위한 보안 헤더(Security Header)(640)를 포함한다.
- <66> 보안 헤더(640)는 다시 타임스탬프(Timestamp)(642), 보안 토큰(Security Token)(644), 암호 키(Encrypted Key)(646) 및 암호화된 서명(Encrypted Signature)(648)을 포함한다.
- <67> 여기서, 타임스탬프(642), 보안 토큰(644), 암호 키(646)는 도 1을 참조하여 설명한 SOAP 메시지의 구성과 동일한 구조 및 기능을 가지므로 여기에서는 설명의 편의를 위하여 별도의 설명을 생략하여도 당업자에 의해 쉽게 이해될 것이다.
- <68> 한편, 보안 헤더(640)에 포함된 암호화된 서명(648)은 XML 디지털 서명 알고리즘을 이용하여 데이터를 서명한 부분을 데이터 암호화시에 사용된 비밀키로 대칭키 알고리즘에 따라 암호화된 것이다.
- <69> 종래의 SOAP 메시지 보안에서 발견된 문제점은 데이터 기밀성의 여부와 상관없이 외부에 서명이 노출되어 있는 상황에서는 제3자에 의해 서명이 교체될 수 있기 때문에, 이러한 서명 교체에 의한 서명 위조를 막기 위해서, 보안 헤더(640)의 서명 부분을 암호화(648)하여 구성한다. 따라서, 제3자는 암호화된 서명(648)을 비밀키가 없이는 쉽게 볼 수 없으므로, 서명을 위

조할 수 없게 된다. 그러나, 수신측에서는 암호화된 서명(648)을 복호화한 다음 서명 검증을 행하므로 SOAP 데이터를 복호화할 수 있게 된다.

<70> 한편, SOAP 본문(660)은 암호 데이터(Encrypted Data)(662)를 포함하며, 이 암호 데이터(662)는 XML 암호 알고리즘(Encryption Algorithm)을 이용하여 SOAP 본문 데이터를 암호화한 부분으로 데이터의 기밀성을 제공하는 것에 대해서는 이미 도 1을 참조하여 설명한 바와 같다.

<71> 도 7은 도 6에 도시된 암호화된 서명(648) 생성 메커니즘에 대한 블록도로, 암호화된 서명 생성 메커니즘은 SOAP 메시지 보안에서 데이터를 암호화하는 비밀키를 사용하여 서명을 암호화하고, 데이터 및 서명 암호화에 사용된 비밀키를 다시 수신자의 공개키로 암호화해서 안전하게 전송하기 위한 메커니즘이다.

<72> 이 메커니즘에서 비밀키(Secret Key)는 대칭키 암호 알고리즘에 사용되는 키를 말한다. 대칭키 암호 알고리즘에서는 암호화나 복호화시에 같은 키를 사용한다. 따라서 암호/복호화를 수행하기 앞서 키 교환 과정이 먼저 수행되어야 한다.

<73> 도 7에 도시된 바와 같이, 암호화된 서명 생성 메커니즘은 SET에서의 전자 봉투 메커니즘을 따랐는데, 디지털 서명(Signature)은 SOAP 본문 데이터와 함께 암호/복호화 속도가 빠른 대칭키 암호 알고리즘에 따라 비밀키(세션키)(720)를 사용하여 암호화(701, 703)된 후 각각 암호 데이터(662)와 암호화된 서명(648)으로 만들어져 각각 SOAP 본문(660)과 보안 헤더(640)에 삽입된다(702, 704).

<74> 데이터와 서명의 암호화에 사용된 비밀키(세션키)(720)는 비대칭키 암호 알고리즘에 따라 수신자의 공개키(710)로 암호화(705)되어 일종의 전자봉투라 할 수 있는 암호 키(646)로 생성되어 SOAP 헤더(620), 특히 보안 헤더(640)에 삽입된다(706).

- <75> 한편, SOAP 메시지 수신자는 자신의 개인키로 보안 헤더(740)의 암호 키(746)에 있는 암호화된 비밀키를 복호화해서 비밀키(세션키)(720)를 얻은 다음, 이 비밀키(세션키)(720)로 암호화된 서명(648)을 복호화하여 본래의 서명문을 얻게 된다.
- <76> 도 8은 도 6에 도시된 SOAP 메시지를 생성하는 흐름도이다.
- <77> 도 8을 참조하면, 먼저 SOAP 본문(660)에 실어 보낼 데이터를 생성한 후, SOAP 메시지 수신자에 대한 라우팅 정보를 구성하여 SOAP 헤더(620)의 라우팅 정보(622)를 생성한다(S710).
- <78> 다음, 보안 헤더(640)의 타임스탬프(642) 및 보안 토큰(644)을 생성한다(S720, S730). 이 때 보안 토큰(644)이 서명된 보안 토큰(Signed Security Token)인 경우엔 인증기관(Certification Authority)에 의뢰하여 얻을 수도 있다. 만약 SOAP 본문 데이터에 제3자에게 공개해서는 안 되는 정보가 있다면, 데이터를 비밀키(720)를 사용하여 암호화(S740)하여 암호 데이터(662)를 생성한 후 SOAP 본문(660)에 삽입함으로써 SOAP 본문 데이터의 기밀성을 유지한다. 여기서, 암호화 과정은 XML 암호 알고리즘을 따른다.
- <79> 다음, 데이터에 대한 무결성 및 신원확인을 위해 디지털 서명(Signature)을 수행하여 서명문을 생성한다(S750). 이 때 디지털 서명은 XML 디지털 서명 알고리즘에 의해 수행된다.
- <80> 그 후, 데이터를 암호화한 비밀키(720)를 사용하여 상기 생성된 서명을 또한 암호화(S760)하여 암호화된 서명(648)을 생성한 후 SOAP 헤더(620)의 보안 헤더(640)에 삽입함으로써 SOAP 메시지의 서명의 제3자에 의한 위조를 방지할 수 있다. 여기서, 암호화 과정은 XML 암호 알고리즘에 따른다.

- <81> 마지막으로, 데이터 암호화와 서명 암호화에 사용된 비밀키(720)는 수신자의 공개키로 암호화하여 암호 키(646)를 생성한 후 보안 헤더(640)에 삽입한다(S770).
- <82> 도 9는 도 6에 도시된 SOAP 메시지를 수신측에서 수신하여 검증하는 과정을 나타낸 흐름도이다.
- <83> 도 9를 참조하면, 먼저 수신자는 전자 서명을 검증하기 위해 SOAP 메시지 헤더(620)나 외부의 인증기관으로부터 인증서를 얻는다(S810).
- <84> 다음, 수신자는 암호화된 디지털 서명(648)을 복호화하기 위해, 수신자의 개인키로 보안 헤더(640)의 암호 키(646)를 복호화하여 비밀키(720)를 획득한다(S820). 이것은 송신자로부터 전송된 SOAP 메시지의 디지털 서명 부분이 비밀키(720)로 암호화되어 있기 때문이다.
- <85> 다음, 획득된 비밀키(720)로 암호화된 서명문을 복호화하여 본래의 서명을 복원한 후 (S830), 상기 단계(S810)에서 얻은 해당 인증서를 가지고 상기 단계(S830)에서 복원된 서명을 검증한다(S840).
- <86> 서명이 검증되고 나면, 상기 단계(S820)에서 이미 복호화된 비밀키(720)로 SOAP 본문 (660)의 암호 데이터(662)를 복호화하여 본래의 데이터를 복원한다(S850).
- <87> 한편, 상기한 바와 같은 본 발명의 실시예에 따른 서명 암호화를 이용한 웹서비스 보안 방법은 프로그램으로 구현되어 컴퓨터로 판독 가능한 형태로 기록 매체(씨디롬, 램, 롬, 플로피 디스크, 하드 디스크, 광자기 디스크 등)에 저장될 수 있다.
- <88> 이상에서 본 발명의 바람직한 실시예에 대하여 상세하게 설명하였지만 본 발명은 이에 한정되는 것은 아니며, 그 외의 다양한 변경이나 변형이 가능하다.

【발명의 효과】

<89> 본 발명에 따르면, SOAP 메시지에 기반한 웹서비스시 SOAP 메시지에 대한 서명 암호화를 수행함으로써, SOAP 메시지 보안에 기초한 웹서비스 보안에서 발생할 수 있는 잠재적인 서명 위조의 위험을 효과적으로 막을 수 있다.

【특허청구범위】**【청구항 1】**

SOAP(Simple Object Access Protocol) 메시지-여기서 SOAP 메시지는 보안 헤더 (Security Header)를 포함하는 SOAP 헤더(Header)와 SOAP 본문(Body)으로 이루어진 SOAP 봉투 (Envelope)를 포함함- 보안에 기초한 웹서비스 보안시 송신자에 의한 상기 SOAP 메시지 생성 방법에 있어서,

- a) 상기 SOAP 메시지의 보안 정보의 재사용을 방지하기 위해 사용되는 타임스탬프 (Timestamp) 및 상기 SOAP 메시지의 보안 관련 정보인 보안 토큰(Security Token)을 생성하여 상기 SOAP 헤더의 보안 헤더에 삽입하는 단계;
- b) 상기 SOAP 메시지를 통해 송신될 데이터를 특정 비밀키를 사용하여 암호화하여 암호 데이터를 생성한 후 상기 SOAP 본문에 삽입하는 단계;
- c) 상기 SOAP 메시지에 대한 무결성 및 신원 확인을 위해 디지털 서명을 수행하여 서명문을 생성하고, 상기 생성된 서명문을 상기 특정 비밀키를 사용하여 암호화하여 암호화된 서명을 생성한 후 상기 SOAP 헤더의 보안 헤더에 삽입하는 단계; 및
- d) 상기 데이터와 서명문의 암호화에 사용된 상기 비밀키를 상기 SOAP 메시지의 수신자의 공개키로 암호화하여 암호 키를 생성한 후 상기 SOAP 헤더의 보안 헤더에 삽입하는 단계를 포함하는 서명 암호화를 이용한 웹서비스 보안시 SOAP 메시지 생성 방법.

【청구항 2】

제1항에 있어서,



상기 b) 단계 및 c) 단계에서, 상기 데이터 및 서명문의 암호화는 대칭키 암호 알고리즘에 따라 수행되는 것을 특징으로 하는 서명 암호화를 이용한 웹서비스 보안시 SOAP 메시지 생성 방법.

【청구항 3】

제1항에 있어서,

상기 d) 단계에서, 상기 비밀키의 암호화는 비대칭키 암호 알고리즘에 따라 수행되는 것을 특징으로 하는 서명 암호화를 이용한 웹서비스 보안시 SOAP 메시지 생성 방법.

【청구항 4】

제1항 내지 제3항 중 어느 한 항에 있어서,

상기 데이터, 서명문 및 비밀키의 암호화는 XML(eXtensible Markup Language) 암호 알고리즘에 따라 수행되는 것을 특징으로 하는 서명 암호화를 이용한 웹서비스 보안시 SOAP 메시지 생성 방법.

【청구항 5】

SOAP(Simple Object Access Protocol) 메시지-여기서 SOAP 메시지는 보안 헤더(Security Header)를 포함하는 SOAP 헤더(Header)와 SOAP 본문(Body)으로 이루어진 SOAP 봉투(Envelope)를 포함함- 보안에 기초한 웹서비스 보안시 수신자에 의한 상기 SOAP 메시지 검증 방법에 있어서,

a) 상기 SOAP 메시지의 서명을 검증하기 위한 인증서를 획득하는 단계;

b) 상기 수신자의 공개키로 상기 SOAP 헤더의 보안 헤더 내에 있는 암호 키를 복호화하여 비밀키를 획득하는 단계;

c) 상기 획득한 비밀키를 사용하여 상기 SOAP 헤더의 보안 헤더 내에 있는 암호화된 서명을 복호화한 후 본래의 서명문을 복원하는 단계;

d) 상기 a) 단계에서 획득한 인증서를 사용하여 상기 c) 단계에서 복원된 서명을 검증하는 단계;

e) 상기 b) 단계에서 획득한 비밀키를 사용하여 상기 SOAP 본문에 있는 암호 데이터를 복호화한 후에 본래의 데이터를 복원하는 단계

를 포함하는 서명 암호화를 이용한 웹서비스 보안시 SOAP 메시지 검증 방법.

【청구항 6】

제5항에 있어서,

상기 a) 단계에서 상기 인증서는 상기 SOAP 헤더의 보안 헤더 내에 있는 보안 토큰 (Security Token)에서 획득되는 것을 특징으로 하는 서명 암호화를 이용한 웹서비스 보안시 SOAP 메시지 검증 방법.

【청구항 7】

제6항에 있어서,

상기 c) 단계 및 e) 단계에서, 상기 암호화된 서명 및 암호 데이터의 복호화는 대칭키 암호 알고리즘에 따라 수행되는 것을 특징으로 하는 서명 암호화를 이용한 웹서비스 보안시 SOAP 메시지 검증 방법.

【청구항 8】

제6항에 있어서,

상기 b) 단계에서, 상기 암호 키의 복호화는 비대칭키 암호 알고리즘에 따라 수행되는 것을 특징으로 하는 서명 암호화를 이용한 웹서비스 보안시 SOAP 메시지 검증 방법.

【청구항 9】

제6항 내지 제8항 중 어느 한 항에 있어서,

상기 암호 키, 암호화된 서명 및 암호 데이터의 복호화는 XML(eXtensible Markup Language) 암호 알고리즘에 따라 수행되는 것을 특징으로 하는 서명 암호화를 이용한 웹서비스 보안시 SOAP 메시지 검증 방법.

【청구항 10】

SOAP(Simple Object Access Protocol) 메시지-여기서 SOAP 메시지는 보안 헤더(Security Header)를 포함하는 SOAP 헤더(Header)와 SOAP 본문(Body)으로 이루어진 SOAP 봉투(Envelope)를 포함함- 보안에 기초한 웹서비스 보안시 송신자에 의한 상기 SOAP 메시지 생성 방법에 있어서,

a) 상기 SOAP 메시지의 보안 정보의 재사용을 방지하기 위해 사용되는 타임스탬프(Timestamp) 및 상기 SOAP 메시지의 보안 관련 정보인 보안 토큰(Security Token)을 생성하여 상기 SOAP 헤더의 보안 헤더에 삽입하는 기능;

b) 상기 SOAP 메시지를 통해 송신될 데이터를 특정 비밀키를 사용하여 암호화하여 암호 데이터를 생성한 후 상기 SOAP 본문에 삽입하는 기능;



c) 상기 SOAP 메시지에 대한 무결성 및 신원 확인을 위해 디지털 서명을 수행하여 서명문을 생성하고, 상기 생성된 서명문을 상기 특정 비밀키를 사용하여 암호화하여 암호화된 서명을 생성한 후 상기 SOAP 헤더의 보안 헤더에 삽입하는 기능; 및

d) 상기 데이터와 서명문의 암호화에 사용된 상기 비밀키를 상기 SOAP 메시지의 수신자의 공개키로 암호화하여 암호 키를 생성한 후 상기 SOAP 헤더의 보안 헤더에 삽입하는 기능을 구현하는 프로그램이 저장된 기록매체.

【청구항 11】

SOAP(Simple Object Access Protocol) 메시지 - 여기서 SOAP 메시지는 보안 헤더(Security Header)를 포함하는 SOAP 헤더(Header)와 SOAP 본문(Body)으로 이루어진 SOAP 봉투(Envelope)를 포함함 - 보안에 기초한 웹서비스 보안시 수신자에 의한 상기 SOAP 메시지 검증 방법에 있어서,

a) 상기 SOAP 메시지의 서명을 검증하기 위한 인증서를 획득하는 기능;

b) 상기 수신자의 공개키로 상기 SOAP 헤더의 보안 헤더 내에 있는 암호 키를 복호화하여 비밀키를 획득하는 기능;

c) 상기 획득한 비밀키를 사용하여 상기 SOAP 헤더의 보안 헤더 내에 있는 암호화된 서명을 복호화한 후 본래의 서명문을 복원하는 기능;

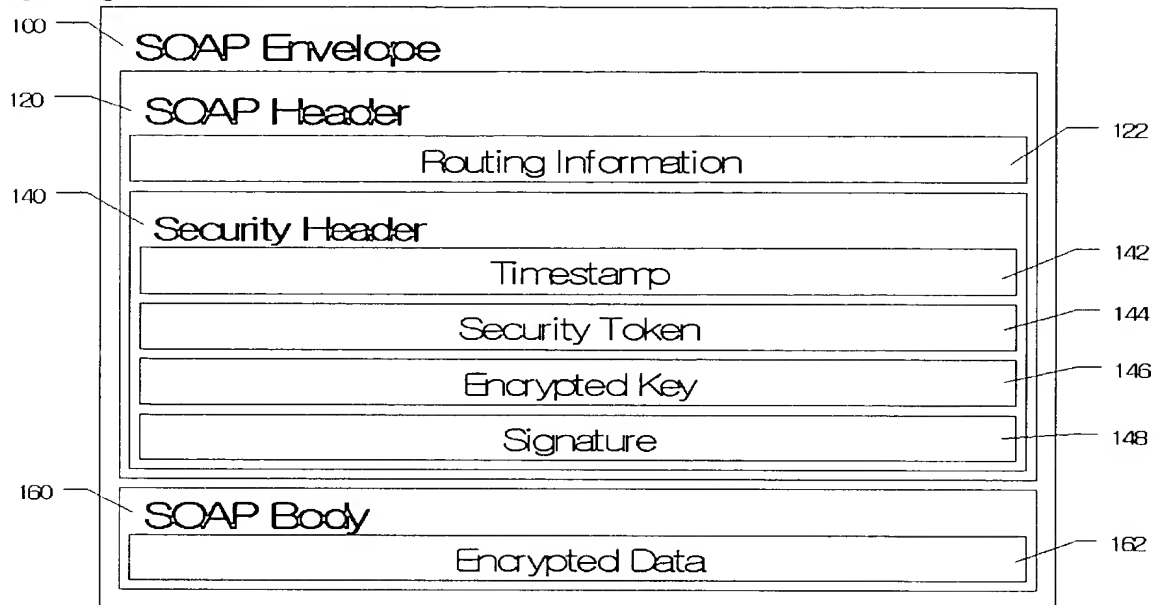
d) 상기 a) 단계에서 획득한 인증서를 사용하여 상기 c) 단계에서 복원된 서명을 검증하는 기능;

e) 상기 b) 단계에서 획득한 비밀키를 사용하여 상기 SOAP 본문에 있는 암호 데이터를 복호화한 후에 본래의 데이터를 복원하는 기능을 구현하는 프로그램이 저장된 기록매체.

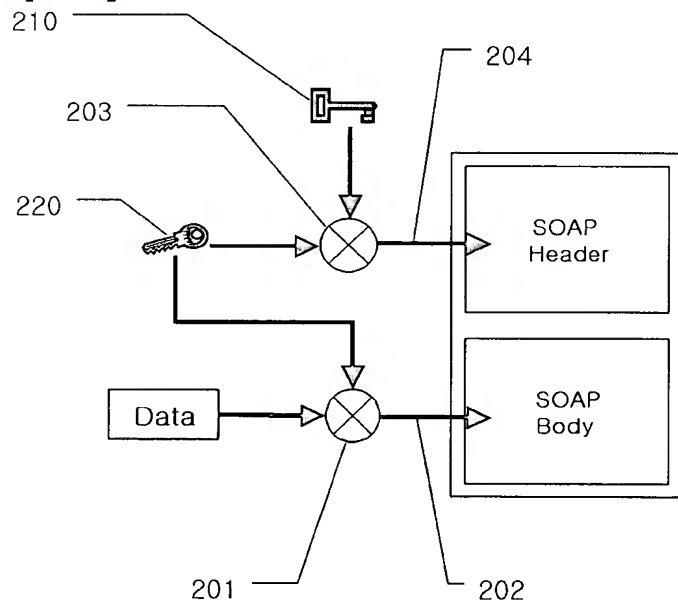


【도면】

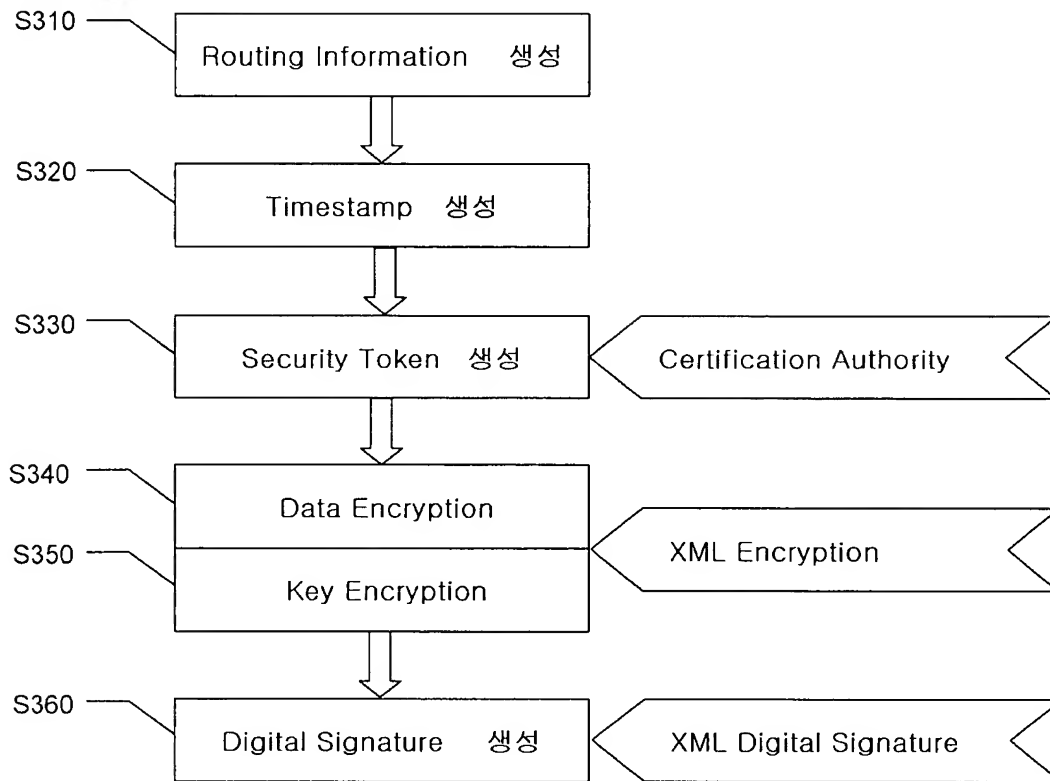
【도 1】



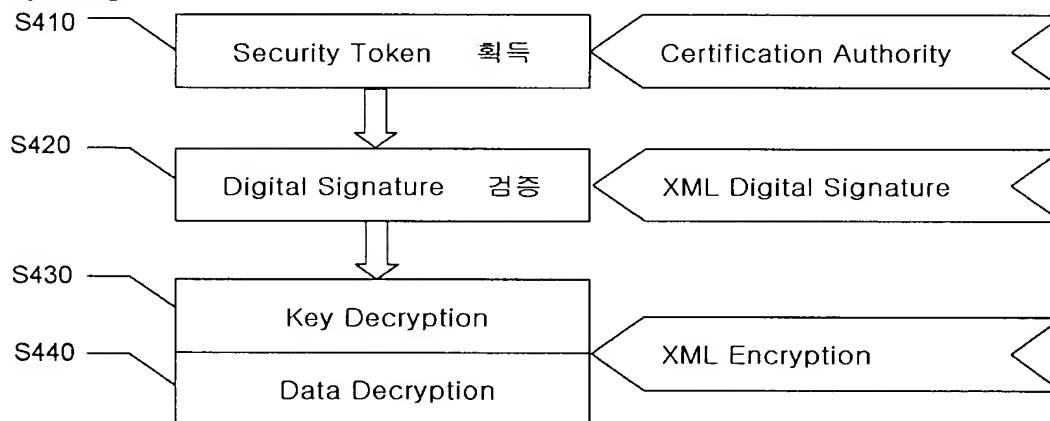
【도 2】



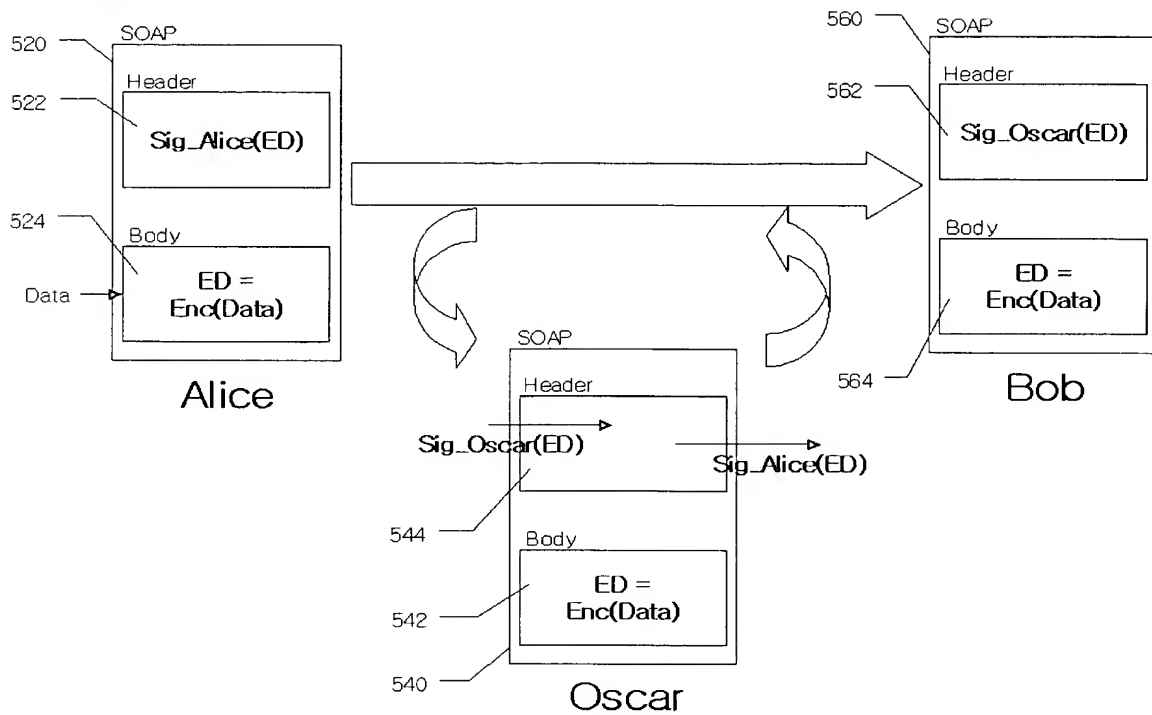
【도 3】



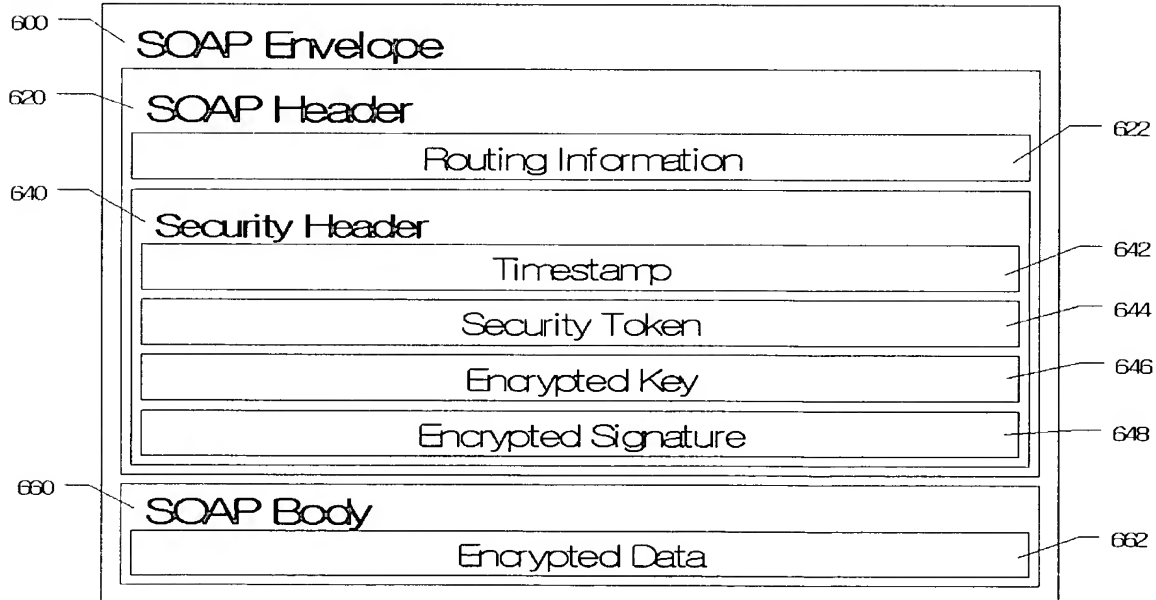
【도 4】



【도 5】

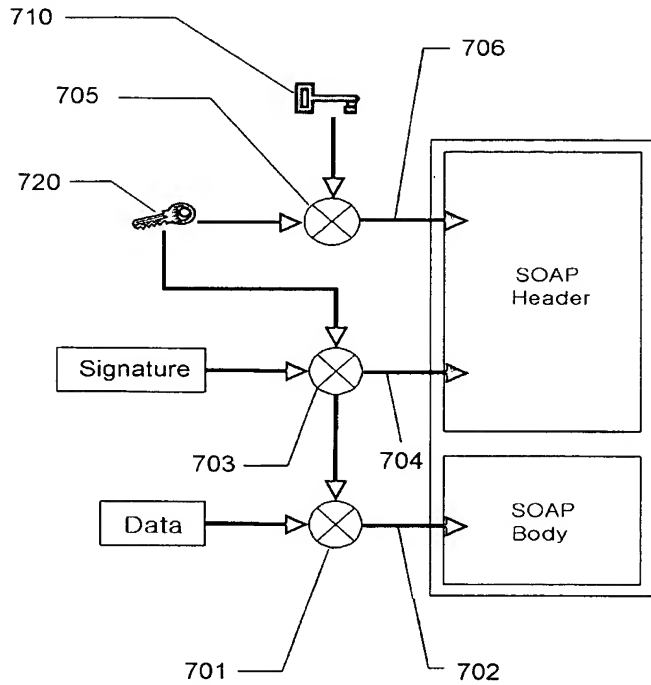


【도 6】





【도 7】



【도 8】

